Félix Clément
Kevin Pronovost
Winner Mazonzika Pindi
Aka Davy Miles Bagui Zabri
Toky Rasolonjatovo

Groupe :00

Mathématiques pour

Informaticiens II

PIF1006

Travail Pratique #3

Cryptographie

Travail présenté à

Adam Joly

Département de mathématiques et d'informatique

Université du Québec à Trois-Rivières

Remis le 20 décembre 2021

Introduction

Nous avons programmé une application console qui nous permet de comprendre les différentes méthodes de programmation de cryptographie On peut y voir, la méthode de chiffrement par bloc CBC (*cypher block chaining*) qui permet de passer d'un bloc de texte clair vers un bloc de texte chiffré en utilisant un vecteur d'initialisation et des méthodes de chiffrement et déchiffrement. Également, le chiffrement par transposition qui consiste à transposer les symboles ou les groupes de symboles d'un message clair à l'intérieur d'un bloc suivant des règles prédéfinies est également utilisé pour la fonction de chiffrement du CBC.

Rôle

Pour ce travail, nous nous sommes dit que nous allions effectuer le travail tous ensemble lors de différentes rencontres sur *Discord*. Nous avons utilisé la fonctionnalité de partage d'écran de cette merveilleuse application afin de pouvoir s'entraider. Ainsi, il n'y a aucun rôle attitré, car pour les raisons évoquées plus haut, nous avons effectué le travail en équipe. Cette façon de travailler a permis à chaque membre de l'équipe d'approfondir ses connaissances sur le langage de programmation *C#*.

Information d'exécution

Le vecteur d'initialisation est déterminé au hasard à chaque fois que l'application est démarré[1]. Tant que l'application n'est pas fermée, le vecteur d'initialisation restera le même. Toutefois, si l'application est quittée et redémarrée, le vecteur d'initialisation sera différent. Nous nous sommes légèrement inspirées du patron ***GOF*** *Singleton* pour générer ce vecteur. S'il est *null*, nous lui donnons une valeur attribuée aux hasards. Sinon, on ne modifie pas ça valeur. La clef de cryptage fonctionne de la manière spécifié le devis du travail. Aucune validation n'est faite sur la validité de la clef. (Il faut entrer les chiffres séparés à l'aide d'espace.)

1. Et que la méthode *Chiffrement()* ou *Déchiffrement()* est appelé pour la première fois.

Information complémentaire

J'ai rajouté une fonctionnalité pour crypter en RSA. C'était mon travail pratique numéro 5 dans mon cours de ***Mathématique discrète*** *au cégep. J'ai renommé le main pour pouvoir l'ajouter à ce programme. Vous sembliez intéressé par la cryptographie alors je pense que ça pourrait peut-être vous intéressé. – Félix*

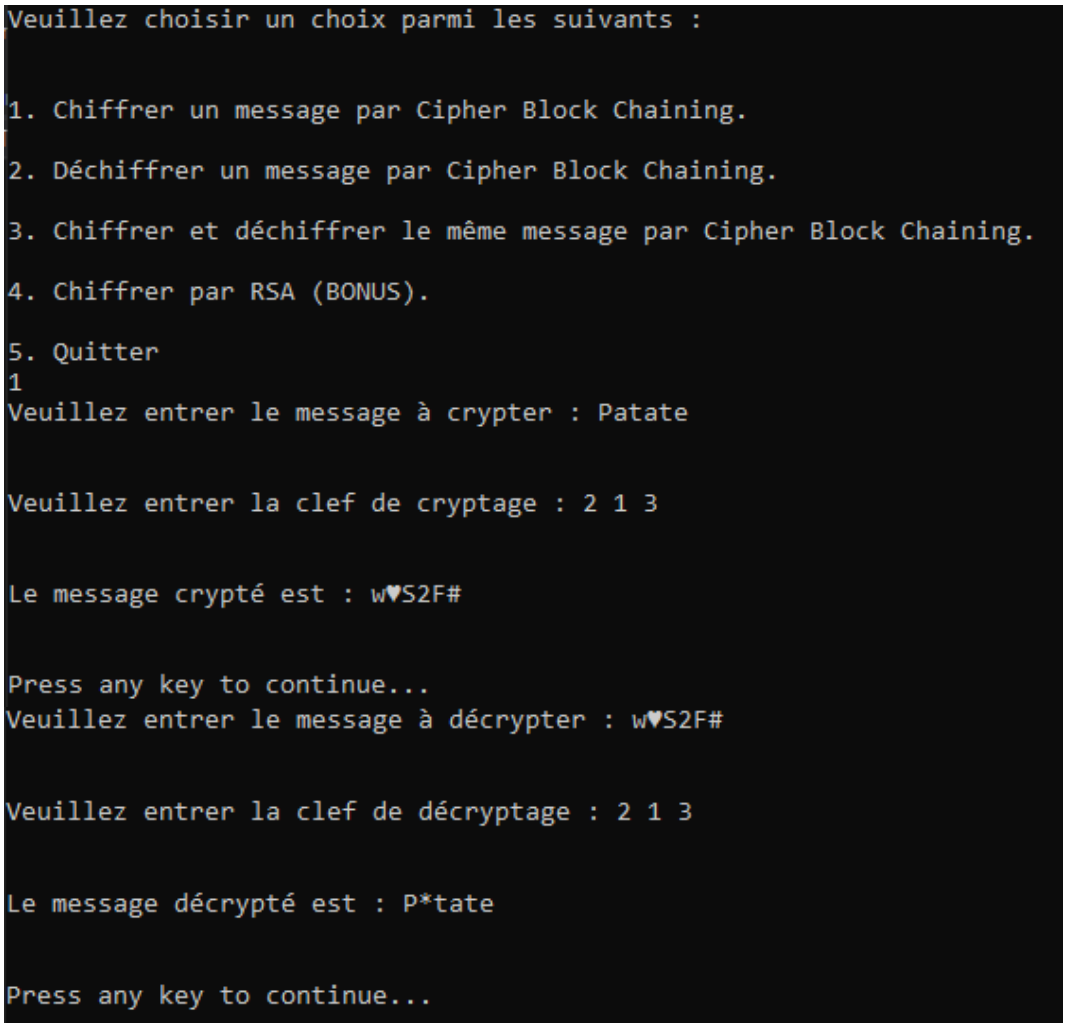
Exemples de RSA :

```
Veuillez entrer le mot que vous voulez crypter :
Patate
Veuillez entrer le paramètre p :
7919
7919 est un nombre premier!
Veuillez entrer le paramètre q :
6553
6553 est un nombre premier!
Veuillez entrer le paramètre e :
11
Le message crypté est : -13715416024572170024572170419430 4
Décryptage du message en cours!
Le message décodé est : Patate
```

```
Veuillez entrer le mot que vous voulez crypter :
Adam est un Super Prof!
Veuillez entrer le paramètre p :
7
7 est un nombre premier!
Veuillez entrer le paramètre q :
13
13 est un nombre premier!
Veuillez entrer le paramètre e :
3
e n'est pas premier avec 72
Veuillez entrer une autre valeur!
Veuillez entrer le paramètre e :
5
Le message crypté est : -261038-39234480-397613-39-1476712375-39-75751431-64
Décryptage du message en cours!
Le message décodé est : Adam est un Super Prof!
```

Pour le premier exemple, il faut faire attention à ne pas mettre d'espace, sinon il peut y avoir une Exception *ArithmeticOverflow* dû aux trops grands nombres utilisés.

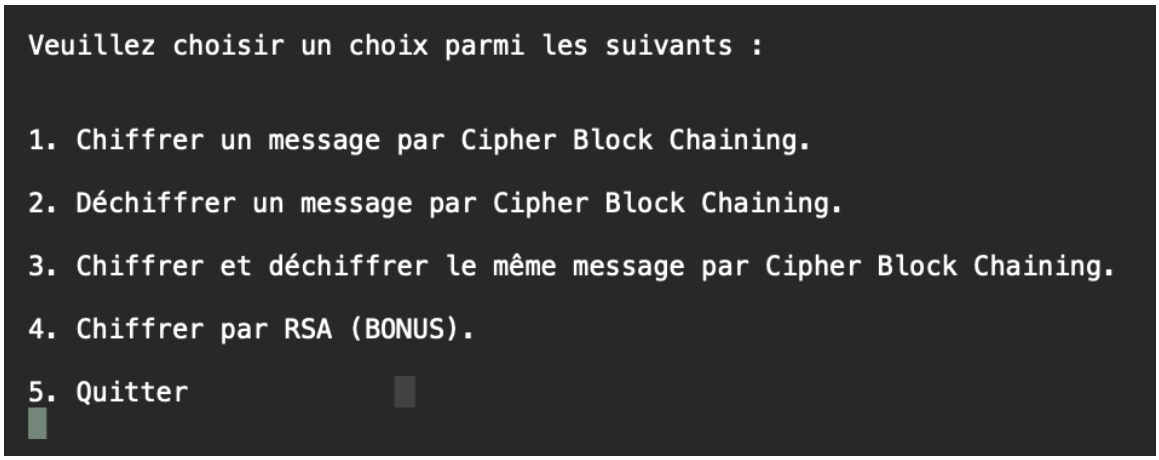
Si nous cryptons et que nous décryptons le même message, mais avec un vecteur d'initialisation différent (soit en redémarrant le programme), nous pouvons constater qu'un seul caractère est mal décrypté. (Dans l'exemple ci-dessous, ce n'est pas le premier à cause de la transposition qui a été appliqué au message.) Ceci nous montre que la méthode CBC n'est pas sécuritaire si une personne sait que le message a été crypté en utilisant cette méthode.



Guide utilisateur

Le menu Principal

Le menu apparaît à l'ouverture de l'application. Il permet à l'utilisateur de choisir s'il veut chiffrer ou déchiffrer un message. C'est commande sont :



Un exemple qui fonctionne avec une clé de transposition quelconque

On crypte et décrypte le message de base : « ce cours de mathématique est très intéressant avec la clé de base 1 4 6 5 3 2.

```
Veuillez choisir un choix parmi les suivants :


1. Chiffrer un message par Cipher Block Chaining.

2. Déchiffrer un message par Cipher Block Chaining.

3. Chiffrer et déchiffrer le même message par Cipher Block Chaining.

4. Chiffrer par RSA (BONUS).

5. Quitter
3
Veuillez entrer le message à crypter : ce cours de mathematique est tres interressant


Veuillez entrer la clef de cryptage : 1 4 6 5 3 2


~e message crypté est : s_-Y*_wmqq$M((M>_+N+N/L(@1EecCc~
 b


Le message décrypté est : ce cours de mathematique est tres interressant


Press any key to continue...
```

Note : parfois, pour une raison obscure, le message crypté modifie les caractères de l'affichage pour dire quel est le message crypté.

Un second exemple qui fonctionne avec une autre clé de transposition avec une quantité différente de nombres;

Ici, je test avec le message « le cours est très palpitant » et une clé de transposition « 3 1 5 2 4 6 7 » plus long et différente.

```
Veuillez choisir un choix parmi les suivants :

1. Chiffrer un message par Cipher Block Chaining.

2. Déchiffrer un message par Cipher Block Chaining.

3. Chiffrer et déchiffrer le même message par Cipher Block Chaining.

4. Chiffrer par RSA (BONUS).

5. Quitter
3
Veuillez entrer le message à crypter : le cours est tres palpitant


Veuillez entrer la clef de cryptage : 3 1 5 2 4 6 7


Le message crypté est : §Â«È»úåçüâÂ§Ô Õõàæ


Le message décrypté est : le cours est tres palpitant


Press any key to continue...
```

Un troisième exemple pour lequel la clé tentée pour le déchiffrement est différente de celle utilisée pour le chiffrement.

Dans cet exemple, ce choisi simplement de prendre la clé de base « 1 4 6 5 3 2 » pour chiffrer le message « bonjour ». Ensuite, on prendre le message crypter et ont choisi une clé de transposition différente « 2 4 6 5 3 1 » qui donne, un résultat non voulu, mais normal dans la situation.

```
Veuillez choisir un choix parmi les suivants :


1. Chiffrer un message par Cipher Block Chaining.

2. Déchiffrer un message par Cipher Block Chaining.

3. Chiffrer et déchiffrer le même message par Cipher Block Chaining.

4. Chiffrer par RSA (BONUS).

5. Quitter
1
Veuillez entrer le message à crypter : bonjour


Veuillez entrer la clef de cryptage : 1 4 6 5 3 2


Le message crypté est : I;NN!!NN$$JJ


Press any key to continue...
```

```
Veuillez choisir un choix parmi les suivants :


1. Chiffrer un message par Cipher Block Chaining.

2. Déchiffrer un message par Cipher Block Chaining.

3. Chiffrer et déchiffrer le même message par Cipher Block Chaining.

4. Chiffrer par RSA (BONUS).

5. Quitter
2
Veuillez entrer le message à décrypter : I;NN!!NN$$JJ


Veuillez entrer la clef de décryptage : 2 4 6 5 3 1


Le message décrypté est : uonjobr


Press any key to continue...
```